Amendments to the Specification:

Page 36, lines 3-8, please amend, as follows:

The second observation is that, if the grantor *A* is the one who encrypts the message *m,* then *A* can keep the random number *k* private and use *B*'s public key $\beta = g^b (\text{mod } p)$, instead of *B*'s private key *b*, to generate the proxy key:

$$\pi = (\beta \cancel{\alpha} \underline{a}^{-1})^k (\text{mod } p),$$

where ~~α~~ *a* is *A*'s ~~public~~ private key. This eliminates the requirement for *B*'s private key *b* (or key exchange between *A* and *B*), and implies that *B* does not have to trust *A*, either.